UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,532	03/26/2004	Akira Yaegashi	SON-2960	7528

23353 7590 11/28/2007
RADER FISHMAN & GRAUER PLLC
LION BUILDING
1233 20TH STREET N.W., SUITE 501
WASHINGTON, DC 20036

EXAMINER	
CUTLER, ALBERT H	

ART UNIT	PAPER NUMBER
2622	

MAIL DATE	DELIVERY MODE
11/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/809,532	YAEGASHI, AKIRA	
	Examiner	Art Unit	
	Albert H. Cutler	2622	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,9,11,12 and 14-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,9,11,12 and 14-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is responsive to communication filed on September 27, 2007. Claims 1-4, 9, 11, 12 and 14-24 are pending in the application. Claims 5-8, 10 and 13 have been cancelled by Applicant.

Response to Arguments

2. Applicant's arguments, see pages 11-14, filed September 27, 2007, with respect to the rejection(s) of claim(s) 1-4, 9, 11, 12 and 14-17 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Hamilton(US 2002/0118837) and Read(US 2004/0085446).

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 18 is rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. Claim 18 describes a computer program stored on a computer readable medium comprising steps. However, said computer program comprising steps could be non-functional material, such as a text file. The Examiner recommends changing claim 18 to read, "A computer program, stored on a computer

readable medium, for making a computer performs the steps of", or something of similar nature to the computer program claimed in claim 17.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 9, 11, 12, 14, 15 and 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Hamilton(US 2002/0118837).

Consider claim 9, Hamilton teaches:

An image pickup apparatus unit(figures 1 and 2) comprising:

an image pickup apparatus(12) having a unique identifying number(serial number, 22) and having an encrypting function for encrypting a picked-up image for transmission to a network(paragraphs 0055-0056); and

a removable recording medium for recording a decryption key(20) for decrypting the image encrypted by said image pickup apparatus and the identifying number of said image pickup apparatus in association with each other(The key(20) and the serial number(22) may be communicated to an authorization center by traditional hard copy methods(i.e. via a removable recording medium), see end of paragraph 0079. The key(20) allows the decryption of images taken by the camera, paragraph 0071.) wherein

said image pickup apparatus(12) receives an encryption key(20) for encrypting said image from a key generating apparatus(See paragraphs 0058, 0068, and 0078. Keys can be generated by the manufacturer or authorization center, by such means as a pseudo-random number generator.).

Consider claim 11, and as applied to claim 9 above, Hamilton further teaches:

said removable recording medium receives the decryption key(20) for decrypting said image from a key generating apparatus(See paragraph 0079. If a decryption key is stored in hard copy form, the decryption key must have been generated by a key generating apparatus. See paragraphs 0058, 0068, and 0078.).

Consider claim 12, and as applied to claim 9 above, Hamilton further teaches that said image pickup apparatus is at least one of a USB camera(paragraph 0049).

Consider claim 14, Hamilton teaches:

A key generating apparatus for generating an encryption key used for encryption processing in transmitting an image(27) via a network(See paragraph 0058, figures 1 and 2. A key(22) is generated by a retailer or manufacturer and stored in a camera(12). The key is used to encrypt images, paragraph 0047. A pseudo-random number generator may be used to generate keys, paragraph 0068.), and a decryption key(paragraph 0071),

wherein said key generating apparatus generates the encryption key(20) for encrypting said image(27) and transmits the encryption key(20) to an image pickup apparatus(12) having a unique identifying number(serial number, 22) and having an encrypting function for encrypting a picked-up image for transmission to the network(paragraphs 0055-0056); and

said key generating apparatus generates the decryption key for decrypting said encrypted image and transmits the decryption key to a removable recording medium for recording said decryption key and the identifying number of said image pickup-apparatus in association with each other(The key(20) and the serial number(22) may be communicated from the retailer or manufacturer(i.e. the key generating apparatus) to an authorization center by traditional hard copy methods(i.e. via a removable recording medium), paragraph 0079. The key(20) allows the decryption of images taken by the camera, paragraph 0071.).

Consider claim 15, and as applied to claim 14 above, Hamilton further teaches that said key generating apparatus has a linking function for linking said image pickup device(12) to said network(Hamilton teaches that the keys can alternatively be generated in an authorization center(14), paragraphs 0068 and 0078. Images(27) are sent to the authorization center(14) from the camera(12), paragraph 0056. The authorization center(14) may then communicate images(27) to a verifying entity(16). Therefore, the authorization center(i.e. key generating apparatus) links the image pickup device to the overall network.).

Consider claim 17, and as applied to claim 14 above, Hamilton further teaches a computer program stored on a computer readable medium, for making a computer function as the key generator of claim 14(See paragraphs 0068. A pseudo random number generator generates keys of desired lengths, such as 128-bits. A computer program stored on a computer readable medium would have to be used to enable the operation and key generation of the pseudo-random number.).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. Claims 1-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Read(US 2004/0066456) in view of Hamilton(US 2002/0118837).

Consider claim 1, Read teaches:

An image transmission system(figure 1) for transmitting an image via a network(internet, 102), said image transmission system(figure 1) comprising:

one or a plurality of image pickup apparatus(104) each having a unique identifier(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0035.);

a key generating apparatus(106) for generating, for each said image, an encryption key for encrypting said image and a decryption key for decrypting said encrypted image(See paragraphs 0026-0029, figures 2 and 3, paragraph 0033. A symmetric encryption key is generated for each image. The image is encrypted using this key. This key is also transmitted over the internet(102) to server(108) to decrypt the transmitted image.);

a viewing apparatus(108, 110) connected with the decryption key and having a decrypting function for decrypting said encrypted image using said decryption key(see figure 3, paragraph 0033), for viewing the image transmitted via said network by said image pickup apparatus(see paragraphs 0037 and 0041); and

an authenticating server(108) for authenticating said image pickup apparatus accessible from said viewing apparatus(The authenticating server(108) is part of the viewing apparatus(108, 110). It authenticates which cameras a user is authorized to view via a user-ID/password, paragraphs 0035-0037.).

However, Read does not explicitly teach that the image pickup apparatuses have an encryption function for encrypting a picked-up image for transmission on said

network. Read also does not explicitly teach that a key is generated for each image pickup apparatus, of a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other, or that the viewing apparatus is connected with a recording medium.

Hamilton is similar to Read in that Hamilton teaches(see figures 1 and 2) transmitting an encrypted image(28) obtained from a camera(20) via a network(see paragraphs 0055-0056). Hamilton also similarly teaches of decrypting the image at a server using a decryption key(paragraph 0057). Hamilton also teaches that each camera has an identifier, although, Hamilton explicitly teaches that said identifier is a unique identifying number(serial number, 22, figure 1).

However, in addition to the teachings of Read, Hamilton teaches that the image pickup apparatus(12) has an encryption function for encrypting a picked-up image for transmission on said network(paragraphs 0055-0056). Hamilton further teaches that a key is generated for each image pickup apparatus(paragraphs 0058, 0068 and 0078). Hamilton additionally teaches a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other(The key(20) and the serial number(22) may be communicated from the retailer or manufacturer(i.e. the key generating apparatus) to an authorization center by traditional hard copy methods(i.e. via a removable recording medium), paragraph 0079.), and that the server("authorization center") is connected with a recording medium(The authorization center can receive a "hard copy" of the key, paragraph 0079.

This key is used for image decryption, paragraph 0057. Because the key is in hard copy form, it would have to be connected with the server.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to perform encryption in the individual cameras using encryption keys unique to each camera as taught by Hamilton instead of performing encryption in a computer and using new encryption keys for each image as taught by Read for the benefit of increasing security by not having un-encrypted images transmitted between the cameras and computer, and providing for an easier, quicker encryption by not having to generate a new encryption key for every single image. It would have been obvious to a person having ordinary skill in the art at the time of the invention to store and deliver the decryption key taught by Read on a removable recording medium as taught by Hamilton, and connect the removable recording medium to a portion of a viewing apparatus as taught by Hamilton for the benefit that the decryption key cannot be intercepted and illegally used over the internet.

Consider claim 2, Read teaches:

An image transmission system(figure 1) for transmitting an image via a network(internet, 102), said image transmission system(figure 1) comprising:

one or a plurality of image pickup apparatus(104) each having a unique identifier(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0035.);

a key generating apparatus(106) for encrypting an image picked up by said image pickup apparatus(104) and transmitting said image to a network(102), and generating a decryption key(See paragraphs 0026-0029, figures 2 and 3, paragraph 0033. A symmetric encryption key is generated for each image. The image is encrypted using this key. This key is also transmitted over the internet(102) to server(108) to decrypt the transmitted image.);

a viewing apparatus(108, 110) connected with the decryption key and having a decrypting function for decrypting said encrypted image using said decryption key(see figure 3, paragraph 0033), for viewing the image transmitted via said network by said image pickup apparatus(see paragraphs 0037 and 0041); and

an authenticating server(108) for authenticating said image pickup apparatus accessible from said viewing apparatus(The authenticating server(108) is part of the viewing apparatus(108, 110). It authenticates which cameras a user is authorized to view via a user-ID/password, paragraphs 0035-0037.).

However, Read does not explicitly teach that of a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other, or that the viewing apparatus is connected with a recording medium.

Hamilton is similar to Read in that Hamilton teaches(see figures 1 and 2) transmitting an encrypted image(28) obtained from a camera(20) via a network(see paragraphs 0055-0056). Hamilton also similarly teaches of decrypting the image at a server using a decryption key(paragraph 0057). Hamilton also teaches that each

camera has an identifier, although, Hamilton explicitly teaches that said identifier is a unique identifying number(serial number, 22, figure 1).

However, in addition to the teachings of Read, Hamilton teaches a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other(The key(20) and the serial number(22) may be communicated from the retailer or manufacturer(i.e. the key generating apparatus) to an authorization center by traditional hard copy methods(i.e. via a removable recording medium), paragraph 0079.), and that the server("authorization center") is connected with a recording medium(The authorization center can receive a "hard copy" of the key, paragraph 0079. This key is used for image decryption, paragraph 0057. Because the key is in hard copy form, it would have to be connected with the server.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to store and deliver the decryption key taught by Read on a removable recording medium as taught by Hamilton, and connect the removable recording medium to a portion of a viewing apparatus as taught by Hamilton for the benefit that the decryption key cannot be intercepted and illegally used over the internet.

Consider claim 3, Read teaches:

An image transmission system(figure 1) for transmitting an image via a network(internet, 102), said image transmission system(figure 1) comprising:

one or a plurality of image pickup apparatus(104) each having a unique identifier(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0035.);

a transmitting apparatus(106) for encrypting an image picked up by said image pickup apparatus(104) and transmitting said image to a network(102)(See paragraphs 0026-0029, figures 2 and 3, paragraph 0033. A symmetric encryption key is generated for each image. The image is encrypted using this key. This key is also transmitted over the internet(102) to server(108) to decrypt the transmitted image.);

a key generating apparatus(106) for generating, for each said image, an encryption key for encrypting said image and a decryption key for decrypting said encrypted image(See paragraphs 0026-0029, figures 2 and 3, paragraph 0033. A symmetric encryption key is generated for each image. The image is encrypted using this key. This key is also transmitted over the internet(102) to server(108) to decrypt the transmitted image.);

a viewing apparatus(108, 110) connected with the decryption key and having a decrypting function for decrypting said encrypted image using said decryption key(see figure 3, paragraph 0033), for viewing the image transmitted via said network by said image pickup apparatus(see paragraphs 0037 and 0041); and

an authenticating server(108) for authenticating said image pickup apparatus accessible from said viewing apparatus(The authenticating server(108) is part of the viewing apparatus(108, 110). It authenticates which cameras a user is authorized to view via a user-ID/password, paragraphs 0035-0037.).

However, Read does not explicitly teach that a key is generated for each image pickup apparatus, of a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other, or that the viewing apparatus is connected with a recording medium.

Hamilton is similar to Read in that Hamilton teaches(see figures 1 and 2) transmitting an encrypted image(28) obtained from a camera(20) via a network(see paragraphs 0055-0056). Hamilton also similarly teaches of decrypting the image at a server using a decryption key(paragraph 0057). Hamilton also teaches that each camera has an identifier, although, Hamilton explicitly teaches that said identifier is a unique identifying number(serial number, 22, figure 1).

However, in addition to the teachings of Read, Hamilton teaches that a key is generated for each image pickup apparatus(paragraphs 0058, 0068 and 0078). Hamilton additionally teaches a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other(The key(20) and the serial number(22) may be communicated from the retailer or manufacturer(i.e. the key generating apparatus) to an authorization center by traditional hard copy methods(i.e. via a removable recording medium), paragraph 0079.), and that the server("authorization center") is connected with a recording medium(The authorization center can receive a "hard copy" of the key, paragraph 0079. This key is used for image decryption, paragraph 0057. Because the key is in hard copy form, it would have to be connected with the server.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to perform encryption using encryption keys unique to each camera as taught by Hamilton instead of performing encryption using new encryption keys for each image as taught by Read for the benefit of providing for an easier, quicker encryption by not having to generate a new encryption key for every single image. It would have been obvious to a person having ordinary skill in the art at the time of the invention to store and deliver the decryption key taught by Read on a removable recording medium as taught by Hamilton, and connect the removable recording medium to a portion of a viewing apparatus as taught by Hamilton for the benefit that the decryption key cannot be intercepted and illegally used over the internet.

Consider claim 4, Read teaches:

An image transmission system(figure 1) for transmitting an image via a network(internet, 102), said image transmission system(figure 1) comprising:

one or a plurality of image pickup apparatus(104) each having a unique identifier(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0035.);

a key generating apparatus(106) for generating, for each said image, an encryption key for said image to encrypt the image and a decryption key(See paragraphs 0026-0029, figures 2 and 3, paragraph 0033. A symmetric encryption key is generated for each image. The image is encrypted using this key. This key is also transmitted over the internet(102) to server(108) to decrypt the transmitted image.);

a viewing apparatus(108, 110) connected with the decryption key and having a decrypting function for decrypting said encrypted image using said decryption key(see figure 3, paragraph 0033), for viewing the image transmitted via said network by said image pickup apparatus(see paragraphs 0037 and 0041); and

However, Read does not explicitly teach that the image pickup apparatuses have an encryption function for encrypting a picked-up image for transmission on said network. Read also does not explicitly teach that a key is generated for each image pickup apparatus, of a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other, or that the viewing apparatus is connected with a recording medium.

Hamilton is similar to Read in that Hamilton teaches(see figures 1 and 2) transmitting an encrypted image(28) obtained from a camera(20) via a network(see paragraphs 0055-0056). Hamilton also similarly teaches of decrypting the image at a server using a decryption key(paragraph 0057). Hamilton also teaches that each camera has an identifier, although, Hamilton explicitly teaches that said identifier is a unique identifying number(serial number, 22, figure 1).

However, in addition to the teachings of Read, Hamilton teaches that the image pickup apparatus(12) has an encryption function for encrypting a picked-up image for transmission on said network(paragraphs 0055-0056). Hamilton further teaches that a key is generated for each image pickup apparatus(paragraphs 0058, 0068 and 0078). Hamilton additionally teaches a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association

with each other(The key(20) and the serial number(22) may be communicated from the retailer or manufacturer(i.e. the key generating apparatus) to an authorization center by traditional hard copy methods(i.e. via a removable recording medium), paragraph 0079.), and that the server("authorization center") is connected with a recording medium(The authorization center can receive a "hard copy" of the key, paragraph 0079. This key is used for image decryption, paragraph 0057. Because the key is in hard copy form, it would have to be connected with the server.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to perform encryption in the individual cameras using encryption keys unique to each camera as taught by Hamilton instead of performing encryption in a computer and using new encryption keys for each image as taught by Read for the benefit of increasing security by not having un-encrypted images transmitted between the cameras and computer, and providing for an easier, quicker encryption by not having to generate a new encryption key for every single image. It would have been obvious to a person having ordinary skill in the art at the time of the invention to store and deliver the decryption key taught by Read on a removable recording medium as taught by Hamilton, and connect the removable recording medium to a portion of a viewing apparatus as taught by Hamilton for the benefit that the decryption key cannot be intercepted and illegally used over the internet.

10. Claims 16, 22, 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hamilton(US 2002/0118837) in view of Read(US 2004/0066456).

Consider claim 16, and as applied to claim 14 above, Hamilton teaches that keys are generated by an external source(see claim 14 rationale). Hamilton does not explicitly teach that said key generating apparatus has a compressing function for compressing the image picked up by said image pickup apparatus.

Read is similar to Hamilton in that Read teaches of a key generating apparatus(106, figure 1, paragraphs 0026-0027, figure 2) in an image transfer system(figure 1).

However, in addition to the teachings of Hamilton, Read teaches that the key generating apparatus(106) is in a personal computer(paragraph 0026) connected to a plurality of cameras(104, figure 1), and that the key generation apparatus(106) compresses the image data(paragraph 0026).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to have the key generating apparatus taught by Hamilton reside in a personal computer, and perform a compression function for compressing the images picked up by said image pickup devices as taught by Read for the benefit that encryption keys can be more readily attained due to their local nature, and compressing images results in less memory being needed to store the images as well as less bandwidth necessary for transmission.

Consider claim 22, Hamilton teaches:

An image pickup apparatus(12, figures 1 and 2) used in an image transmission system(figure 1) for transmitting an image(28) via a network(paragraph 0056), said image pickup apparatus(12) comprising:

a recording unit(22) for recording a unique identifying number(serial number, paragraph 0048);

an encrypting unit for encrypting a picked-up image(paragraph 0055); and

a communicating unit(23, paragraph 0049, not shown in drawings) for transmitting said encrypted image to a viewer(verifying entity, 16, paragraphs 0056-0057).

However, Hamilton does not explicitly teach that the viewer has been authenticated by an authentication server and is permitted to receive encrypted images from the image pickup apparatus.

Read is similar to Hamilton in that read teaches an image transmission system(figure 1) for transmitting an image via a network(internet, 102), said image transmission system(figure 1) comprising one or a plurality of image pickup apparatus(104) each having a unique identifier(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0036.).

However, in addition to the teachings of Hamilton, Read teaches that the viewer has been authenticated by an authentication server and is permitted to receive encrypted images from the image pickup apparatus(An authenticating server(108) is part of a viewing apparatus(108, 110). It authenticates which cameras a user is authorized to view via a user-ID/password, paragraphs 0035-0037.).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to include an authenticating server as taught by Read to permit or prohibit viewers from receiving the encrypted images taught by Hamilton for the benefit of improving security by only allowing viewers access to authorized and appropriate images.

Consider claim 23, and as applied to claim 22 above, Hamilton further teaches that said communicating unit includes a receiving unit for receiving an encryption key for encrypting said image from a key generating apparatus(paragraphs 0058, 0068 and 0078).

Consider claim 24, and as applied to claim 22 above, Hamilton further teaches that said communicating unit includes at least one of a USB port(see paragraph 0049).

11. Claims 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Park(US 2004/0085446) in view of Read(US 2004/0066456) in view of Oishi(Us 6,999,588).

Consider claim 18, Park teaches:

A computer program, stored on a computer readable medium(Park discusses the use of a stored control program in paragraph 0008), comprising the steps of:

initializing a image transmission system, comprising connecting an image pickup apparatus(100, figure 1, 110, figure 2) to a key generating apparatus(The image pickup apparatus(110) is connected to an encryption unit(130), which is detailed in figure 4. The encryption unit(130) comprises a key generating apparatus(132) which generates keys for the video data encrypting device(133). See paragraphs 0069 and 0075.);

transmitting an identifying number from the image pickup apparatus to the key generating apparatus(The key generating apparatus stores keys that are associated with received unique camera numbers. See paragraphs 0069 and 0075);

registering the identifying number(115) from the image pickup apparatus(110, 100) at the key generating apparatus(paragraphs 0069 and 0075);

generating an encryption and decryption key unique to the image pickup apparatus(See paragraphs 0069 and 0075 for generating encryption keys unique to image pickup apparatuses. See figure 8 for the decryption unit. The decryption unit contains a key data supplier(322) which stores the same data as key data supplier(132). See paragraphs 0086-0087 for generating decryption keys unique to image pickup apparatuses.);

connecting the image pickup apparatus(100, figure 1, 110, figure 2) to a viewing apparatus(500, See figures 1 and 2, paragraphs 0068 and 0070);

comparing the identification number(115) stored in the receiving device(300) to the identifying number(115) of the image pickup apparatus(100, See paragraphs 0086 and 0087.);

obtaining the decryption key(paragraph 0086);

decrypting images received from the image pickup device using the decryption key(paragraphs 0086-0087);

displaying the decrypted images on the viewer(500, paragraphs 0068 and 0070).

However, Park does not explicitly teach registering an identifying number of an image pickup device at an authentication server, then requesting that the authentication server authenticate a user and authenticate that a user can access the image pickup device, or authenticating the user and image pickup apparatus in response to the requesting step.

Read is similar to Park in that Read teaches an image transmission system(figure 1) for transmitting an image via a network(internet, 102), said image transmission system(figure 1) comprising a plurality of image pickup apparatus(104), each having a unique identifier(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0036.). Read also similarly teaches of viewing a transmitted image(paragraphs 0037 and 0041), and of performing encryption and decryption operations(figures 2 and 3).

However, in addition to the teachings of Park, Read teaches registering an identifying number of an image pickup device(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0036.) at an authentication server(108, paragraphs 0035-0036), then requesting that the authentication server(108) authenticate a user and authenticate that a user can access the image pickup device(paragraphs 0035 and 0036), and authenticating the user and image pickup apparatus in response to the requesting step(paragraph 0037).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to include an authenticating server as taught by Read to permit or prohibit viewers from receiving the encrypted images taught by Park for the benefit of improving security by only allowing viewers access to authorized and appropriate images.

However, the combination of Park and Read does not explicitly teach that the decryption keys associated with the image pickup apparatus identifying numbers are stored in a memory card.

Oishi is similar to Park and Read in that Oishi teaches an image pickup apparatus(100, figure 1) containing an image pickup unit(1) and an encryption unit(5), said image pickup apparatus(100) transmitting encrypted images to an image processing apparatus(200).

However, in addition to the teachings of Park and Read, Oishi teaches that the image pickup apparatus(100) is connected via an interface to a memory card(20, column 6, lines 9 and 10), that a decryption key associated with a specific image pickup apparatus is stored in the memory card(column 7, line 40 through column 8, line 3), and that the decryption key is obtained by the image processing device(200) and used for decryption of the transmitted image data(see column 6, lines 10-17, column 7, line 67 through column 8, line 3, column 10, lines 11-18).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to store decryption keys associated with specific image pickup apparatuses as taught by the combination of Park and Read on a memory card

as taught by Oishi for the benefit of protecting the decryption key from being obtained by illegal users from the image input apparatus(Oishi, column 8, lines 59-64).

Consider claim 19, and as applied to claim 18 above, Park does not explicitly teach accessing the authentication server from a viewing apparatus using a username and password.

However, Read teaches accessing the authentication server from a viewing apparatus using a username and password(paragraph 0035).

Consider claim 20, Park teaches:

An image transmission system for transmitting an image via a network(figures 1 and 2), comprising:

an image pickup apparatus(100, figure 1, 110, figure 2) connected to a key generating apparatus(The image pickup apparatus(110) is connected to an encryption unit(130), which is detailed in figure 4. The encryption unit(130) comprises a key generating apparatus(132) which generates keys for the video data encrypting device(133). See paragraphs 0069 and 0075.), comprising:

a recording unit(132) for storing an identifying number and an encryption key from the key generating apparatus(paragraphs 0069 and 0075);

the key generating apparatus, comprising:

a recording unit(132) for storing the identifying number(115) from the image pickup apparatus(110, paragraph 0075);

an encryption key generation unit for generating an encryption and decryption key unique to the image pickup apparatus(See paragraphs 0069 and 0075 for generating encryption keys unique to image pickup apparatuses. See figure 8 for the decryption unit. The decryption unit contains a key data supplier(322) which stores the same data as key data supplier(132). See paragraphs 0086-0087 for generating decryption keys unique to image pickup apparatuses.);

an image viewer(500, See figures 1 and 2, paragraphs 0068 and 0070) comprising:

an interface for connecting the image pickup apparatus to the viewing apparatus(See paragraphs 0068 and 0070);

an interface for obtaining the decryption key(paragraph 0086);

a decrypting unit(320, figure 2, figure 8) for decrypting the images received from the image pickup device using the decryption key(paragraphs 0086-0087);

a display unit(500) for displaying the decrypted images on the viewer(paragraphs 0068 and 0070).

However, Park does not explicitly teach a network interface for registering the identifying number from the image pickup apparatus at an authentication server, an authentication server for authenticating the user and image pickup apparatus in response to an authentication request, or an interface for requesting that the authentication server authenticate a user and authenticate an image pickup device accessible by the user.

Read is similar to Park in that Read teaches an image transmission system(figure 1) for transmitting an image via a network(internet, 102), said image transmission system(figure 1) comprising a plurality of image pickup apparatus(104), each having a unique identifier(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0036.). Read also similarly teaches of viewing a transmitted image(paragraphs 0037 and 0041), and of performing encryption and decryption operations(figures 2 and 3).

However, in addition to the teachings of Park, Read teaches registering an identifying number of an image pickup device(Cameras have unique identifiers so that a user can be permitted to or restricted from viewing certain cameras, paragraph 0036.) at an authentication server(108, paragraphs 0035-0036), then requesting that the authentication server(108) authenticate a user and authenticate that a user can access the image pickup device(paragraphs 0035 and 0036), and authenticating the user and image pickup apparatus in response to the requesting step(paragraph 0037).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to include an authenticating server as taught by Read to permit or prohibit viewers from receiving the encrypted images taught by Park for the benefit of improving security by only allowing viewers access to authorized and appropriate images.

However, the combination of Park and Read does not explicitly teach that the decryption keys associated with the image pickup apparatus identifying numbers are stored in a removable storage medium.

Oishi is similar to Park and Read in that Oishi teaches an image pickup apparatus(100, figure 1) containing an image pickup unit(1) and an encryption unit(5), said image pickup apparatus(100) transmitting encrypted images to an image processing apparatus(200).

However, in addition to the teachings of Park and Read, Oishi teaches that the image pickup apparatus(100) is connected via an interface to a memory card(i.e. a removable storage medium, 20, column 6, lines 9 and 10), that a decryption key associated with a specific image pickup apparatus is stored in the memory card(column 7, line 40 through column 8, line 3), and that the decryption key is obtained by the image processing device(200) and used for decryption of the transmitted image data(see column 6, lines 10-17, column 7, line 67 through column 8, line 3, column 10, lines 11-18).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time of the invention to store decryption keys associated with specific image pickup apparatuses as taught by the combination of Park and Read on a removable storage medium as taught by Oishi for the benefit of protecting the decryption key from being obtained by illegal users from the image input apparatus(Oishi, column 8, lines 59-64).

Consider claim 21, and as applied to claim 20 above, Park does not explicitly teach the authentication server authenticates the user of the viewing apparatus using a username and password associated with the image pickup apparatus.

However, Read teaches the authentication server authenticates the user of the viewing apparatus using a username and password associated with the image pickup apparatus(paragraph 0035).

Conclusion

12. The rejection previously made to claim 17 under 35 U.S.C. 101 by the Examiner is hereby removed in view of Applicant's response.

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Naruto et al.(US 2003/0026434) teach of a memory card storing encryption keys(see abstract), and of a memory storing unique camera numbers in association with decryption keys(see figure 11, paragraphs 0140 and 0141).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Albert H. Cutler whose telephone number is (571)-270-1460. The examiner can normally be reached on Mon-Fri (7:30-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ngoc-Yen Vu can be reached on (571)-272-7320. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AC

NGOC-YEN VU
SUPERVISORY PATENT EXAMINER